AMENDMENTS TO THE SPECIFICATION

Please amend the specification on page 10 line 21 through page 11 line 7 as follows:

Following key generation and verification, the system moves to a decision state 86, where the result of the key verification of block 84 is checked. If the key is verified as good, the system moves to block 88, and the key is used to encrypt and decrypt data during data storage and retrieval operations. There are several reasons why key verification might fail. An error in reading the hardware identifier may cause faulty key generation. Tampering with the logic circuit 50 may also result in incorrect key generation. Additionally, key verification may fail because required operator input to be used in key generation has not yet been entered by a user. Thus, a failure of key verification may force user input. This is illustrated in Figure 4 by the fact that if, at decision state 86, the key has not been verified as good, the system moves to [[a]] another decision state 90. At decision state 90, the system determines whether or not user input should be accepted and used in the key generation process. If the system determines that operator input should be accepted, the system moves to block 92, where the input is read. The system then loops back to block 84, where the key is generated using both the operator input and the retrieved identification code, and is again verified against the stored CRC or checksum field. If the operator input was the correct password, the key will be verified as good at the next iteration of decision block 86, and at block 88, the key will be used to encrypt and decrypt data as described above.